Ungeklärte Verhaltensweisen von Mitarbeitern – was macht der Maier den ganzen Tag?

Die Stimmung in der Firma ist schlecht, die Mitarbeiter haben Angst ihre Anstellung zu verlieren und nichts läuft mehr rund: Alles dauert länger wegen der Kurzarbeit, keiner fühlt sich zuständig, der Toner im Drucker ist wieder leer, das Internet langsam, die Datenzugriffe funktionieren nicht mehr richtig und die Passwörter hat auch jemand geändert. Nichts ist, wie es war und keiner ist zuständig. Alles murrt und ist verstimmt. Wirtschaftskrise: Kurzarbeit, Entlassungen und Betriebsschließungen. Ein fruchtbarer Boden für Personen, die versuchen auch in wirtschaftlich schlechten Zeiten „ihre Schäfchen ins Trockene zu bringen".

Gefahrenpotential Mitarbeiter

Dank gezielter Marketing-Kampagnen sind die meisten Unternehmen wenigstens mit einer Basis-Sicherheit ausgestattet: Virenscanner, Firewall und Backup. Nur wenige Unbelehrbare verzichten fahrlässig auf diese grundlegenden Techniken zur Absicherungen ihrer Daten. Es lässt sich auch trefflich darüber streiten, wie sinnvoll diese Techniken eingesetzt werden, aber sie bilden die erste Hürde für Angriffe auf die Unternehmensdaten.
Da der Mensch grundsätzlich dazu neigt, den Weg des geringsten Widerstands zu gehen, wird an der Stelle angegriffen, die das größte Unsicherheitspotential bietet: am Mitarbeiter. Ein Unternehmensnetzwerk ist immer nur so gut, wie sein schwächstes Glied. Der Mitarbeiter, insbesondere der unzufriedene Mitarbeiter, stellt hier ein großes Gefahrenpotential dar. Oft bezahlen Unternehmer die mangelnde Sicherheit der Arbeitsplätze mit Illoyalität und kleinen Diebstählen. Ganz groß in der Presse waren die Entlassungen nach Frikadellen-Diebstahl oder Veruntreuung von Getränke-Pfand-Bons.
Obwohl seit dem 1. September 2009 laut Bundesdatenschutzgesetz eine Meldepflicht für Datendiebstähle besteht, scheuen sich die Unternehmen diese offen zu bekennen oder wissen nicht einmal, dass sie bestohlen wurden. Offensichtlich werden die Verluste aus diesen Datendiebstählen lieber hingenommen, als der mögliche Imageverlust. Dieses Verhalten ermöglicht aber professionellen Datendieben, mit der gleichen Technik mehrere Firmen zu schädigen. Datenschützer befürchten, dass im Jahre 2009 jedes zweite Unternehmen einen Datendiebstahl erlitten habe und insgesamt 79% aller Unternehmen schon mit entwendeten Daten Probleme hatte.

Klassischer Datendiebstahl

Ein Hersteller von Ersatzteilen für Motorräder hatte das Problem, dass er seine patentierten Bauteile von einem Mitanbieter zu deutlich günstigeren Preisen auf einer Messe entdeckt hat. Besonders auffällig war, dass ein ehemaliger Mitarbeiter von ihm in dieser Firma vorübergehend beschäftigt, aktuell aber auf Arbeitssuche war. An dieser Stelle beauftragte der Unternehmer einen Sachverständigen, der klären sollte, in wie weit die Ersatzteile der Konkurrenz tatsächlich auf seinen Zeichnungen und Patenten fußten und wie die Daten dorthin kommen konnten. Während der Schadenersatzklage gegen das Konkurrenzunternehmen bekam er unerwartet Hilfe, mit der er nicht gerechnet hatte: sein ehemaliger Mitarbeiter fand keine Beschäftigung und schlug seinem ehemaligen Arbeitgeber einen Deal vor: gegen eine entsprechende Leistung sei er bereit als Zeuge zu bestätigen, dass er die Unterlagen entwendet habe um sie

an den Mitanbieter zu verkaufen. Um das Verfahren abzukürzen und den Prozess zu seinen Gunsten zu entscheiden, nahm er das Angebot seines Ex-Mitarbeiters an. Der Unternehmer bekam Recht und einen angemessenen Schadensersatz, allerdings „revanchierte" er sich bei seinem hilfreichen Mitarbeiter nicht mit einer Erfolgsprämie und einer Anstellung auf Lebenszeit, sondern einer Anzeige wegen Veruntreuung und Wirtschaftsspionage.
Ohne die Aussage seines untreuen Mitarbeiters hätte er nur schwer beweisen können, dass die Konstruktionszeichnungen aus seinem Hause stammten. In seinem Betrieb waren keinerlei Maßnahmen getroffen worden, um diese vertraulichen Daten vor unberechtigten Zugriffen zu schützen und Zugriffe von berechtigten oder nicht berechtigten Personen zu protokollieren.
Ein zweiter Fall, der aber für den Datendieb ohne Folgen blieb, ereignete sich vor bereits 10 Jahren in Süddeutschland. Ein Unternehmen beklagte sich bei seinen Sicherheits-Beratern, dass Firmeninternes im Internet in den unterschiedlichsten Foren zu finden sei und sie vermuteten einen Hacker. Das System wurde geprüft, Mitarbeiter überprüft und verschärfte Sicherheitsmaßnahmen für Mitarbeiter getroffen. Nichts änderte sich und schließlich beschlossen zwei Vorstände die Firma aufgrund der schlechten Marktlage zu verlassen. In Rekordzeit stampften sie ein Konkurrenzunternehmen aus dem Boden und hatten die gleichen Kunden wie die alte Firma. Erst Wochen später viel den verbleibenden Vorstandskollegen auf, dass die verstärkten Sicherheitsrichtlinien nicht für den Vorstand galten und die Firmenlaptops auch nicht zurück gegeben wurden.

Motivation der Computerkriminalität
Das digitale Verbrechen ist in Unternehmen immer mehr auf dem Vormarsch, besonders, wenn die Zukunft des Unternehmens in den Sternen steht. Die Gründe hierfür sind vielfältig. Eine Rolle spielt sicher die Tatsache, dass bei virtuellen Verbrechen die Hemmschwelle des Einzelnen niedriger liegt, als bei Kapitalverbrechen. Eine Datei widerrechtlich zu kopieren, zu manipulieren oder aus dem Unternehmen zu schmuggeln erfordert weniger kriminelle Energie, als eine Bank zu überfallen oder einen Einbruch zu begehen. Zudem ist es vermeintlich leichter, seine Spuren zu verwischen oder zu manipulieren. Im Internet und in einschlägigen Zeitschriften werden Programme und Tipps veröffentlicht, um Daten auszuspionieren und Systeme so zu manipulieren, dass sie leicht Opfer von Angriffen werden können.
Nicht nur „Hobby"-Wirtschaftsspione sind am Werk, sondern auch professionell ausgebildete Fachleute, die im Auftrag von Konkurrenz-Unternehmen oder Geheimdiensten auf der Suche nach wirtschaftlich interessanten Daten sind. Dabei sind nicht nur die Regierungen der Russischen Förderation oder China tätig, sondern auch die Geheimdienste aus anderen Ländern.
"Für einige Nachrichtendienste nehmen Aufklärungsziele im Bereich von Wirtschaft, Wissenschaft und Technik einen zunehmend breiteren Raum ein. Technologisch weniger entwickelte Staaten spähen eher technisches Know-how aus, um Kosten für die eigene Forschung und Entwicklung sowie mögliche Lizenzgebühren zu vermeiden. Höher entwickelte Staaten interessieren sich dagegen für Produktideen, komplexe Fertigungstechniken sowie für Unternehmens- und Marktstrategien." (Verfassungsschutzbericht 2008 Seite 309ff) Ganz gleich, welcher Art der Angriff auf Unternehmensgeheimnisse ist, der Schaden für das Unternehmen ist kaum abzuschätzen.

Entdeckte Verbrechen
In vielen Fällen ist bei den Mitarbeitern das kriminelle Potential zwar vorhanden, doch mangelt es in der Ausführung und an technischem Wissen. Der Versuch

eines Vertriebsmitarbeiters, sich mit seinen Kundendaten bei der Konkurrenz zu bewerben scheiterte aus einem puren Zufall: Am Wochenende beschloss ein Administrator, fällige Wartungsarbeiten zu erledigen. Während er dies tat, fiel ihm auf, dass der Druckserver am Rande seiner Kapazität läuft und extrem große und viele Druckaufträge in der Warteschlange standen. Für diesen Wochentag und in dieser Menge waren Druckaufträge ungewöhnlich, also ging er der Sache nach und stellte fest, dass die Daten aus dem Vertrieb stammten. Eilens begab er sich in den Druckerraum und traute seinen Augen nicht. In den Druckern fanden sich die Ausdrucke aller Kundendaten aus dem CRM-System. Mit einem gewissen Sinn für Humor und der Möglichkeit die Schließanlage der Firma umzuprogrammieren, veranlasste er eine Sperrung des Druckerraums und wartete in der Nähe um den druckwütigen Mitarbeiter zur Rede zu stellen, was auch gelang. Die Firma hat heute eine ausgeklügelte Rechtevergabe und Überwachung und der Mitarbeiter viel Zeit für seine Familie.
Etwas geschickter stellte sich eine junge Dame in einer Anwaltskanzlei an. Als langjährige Mitarbeiterin genoss sie das volle Vertrauen ihres Chefs und erledigte den Zahlungsverkehr der Kanzlei. Durch akute Geldnöte getrieben ersann die Dame folgende Möglichkeit, ihre Kasse wenigstens vorübergehend aufzubessern: sie überwies sich einen stattlichen Betrag und gab, um nicht entdeckt zu werden, die PIN des Kontos danach mehrfach falsch ein. Der Zugang wurde gesperrt. Es wurde eine neue PIN beantragt, die sie auch gleich für ihre Zwecke nutzte und lies sie wieder sperren. Das Spiel war für ihren Chef zwar nervtötend, aber nicht auffällig. Er ärgerte sich über die entsprechende Online-Bank und drohte mit rechtlichen Schritten. Erst als die Dame Urlaub hatte (Geld war ja jetzt da), bekam der Chef seine neubeantragte PIN als erster in die Hand und konnte problemlos den Kontostand abfragen. Danach war ihm klar, warum die PIN immer gesperrt war, wenn er auf sein Firmenkonto zugreifen wollte. Auch hier trennten sich die Parteien, allerdings weniger einvernehmlich.

Möglichkeiten zur Verhinderung von Datendiebstählen
Hier sind Administratoren mehr gefragt denn je. Zu den täglichen Wartungsarbeiten kommt nun auch die Suche nach verändertem oder auffälligem Benutzerverhalten. Ein Themengebiet, das IT-Verantwortliche oft vernachlässigen, da meist die Zeit für weiterführende überwachende Tätigkeiten recht knapp bemessen ist und man sich immer in der Grauzone von Systemüberwachung und Datenschutz befindet. Außerdem scheuen sich viele Administratoren davor, den Kollegen hinterher zu spionieren. Welcher Schaden jedoch für das Unternehmen entstehen und welche Auswirkungen das möglicherweise auf den eigenen Job haben kann, wird übersehen. Ein Security-Consultant meinte in einem Gespräch scherzhaft: „Wenn der Administrator von der Belegschaft nicht mehr gegrüßt wird, dann ist das Netzwerk sicher!" Ob das immer ein Merkmal ist, sei dahingestellt, doch zeigt dieser Ausspruch, dass sich Administratoren durchaus unbeliebt machen müssen, um ihr Netzwerk zu schützen. Oft aber werden sie – nicht selten von der Unternehmensleitung selbst- gezwungen, Funktionalität über Sicherheit zu stellen.
Eine Möglichkeit ist hier die Installation von Arbeitszeiterfassung, Videoüberwachung von sensiblen Bereichen, Monitoring-Programmen, NAC-Systemen und ausgeklügelten Zugriffberechtigungen. Doch jedes System ist so sicher wie seine schwächste Stelle – und die ist (meistens) der Mensch.